## REMARKS/ARGUMENTS

The Examiner objects to claim 7, which has been amended to overcome the objection.

The Examiner rejects claims 1-11, 13-24, and 26-36 under 35 U.S.C.§102(b) as being anticipated by Herr-Hoyman et al. (U.S. Patent 5,727,156) and claims 12 and 25 under 35 U.S.C.§103(a) as being unpatentable over Herr-Hoyman and further in view of Huang et al. (U.S. Patent 6,571,245).

Applicants respectfully traverse the Examiner's rejections. The cited references fail to teach or suggest at least the following italicized features:

> 36. A method of communication data between a first computing device and a second computing device, the method comprising:
>
> (a) providing a display to a user, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields;
>
> (b) receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, *wherein the first datum is confidential to the user and the second datum is non-confidential to the user*;
>
> (c) *identifying that the first datum is confidential and the second datum is non-confidential;*
>
> (d) *the first computing device communicating, to the second computing device, the first datum with encryption; and*
>
> (e) *the first computing device communicating, to the second computing device, the second datum without encryption, wherein steps (d) and (e) occur at least substantially simultaneously.*
>
> 40. A system for communicating data between first and second computing devices, comprising:
>
> (a) a first computer device operable to communicate data, the first computer device comprising:
>
> a user display, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields;
>
> means for receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and

second input fields, respectively, of the display, *wherein the first datum is confidential to the user and the second datum is non-confidential to the user*; and

*means for identifying that the first datum is confidential and the second datum is non-confidential*; and

(b) a second communication device in communication with the first communication device, *wherein the first computing device communicates, to the second computing device, the first datum with encryption and the second datum without encryption.*

44. A method of communicating data between a first computing device and a second computing device, the method comprising the steps of:

at a first computing device, receiving input information from a display to a user, the input information comprising at least first and second datum corresponding respectively to at least first and second user input fields;

at the first computing device, *determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user*;

*the first computing device communicating the first datum of the message to a second computing device with encryption of the first datum; and*

*the first computing device communicating the second datum of the message to the second computing device without encryption of the second datum.*

45. A data communication system comprising:

first and second computing devices, wherein:

the second computing device is operable to provide a display to a user, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields and receive, from the user, a message corresponding to the display, wherein a first datum refers to the first input field and a second datum to the second input field of the display; and

the first computing device is operable to communicate information to the second computing device responsive to a request from the second computing device to the first computing device, *the information including a procedure that causes the second computing device communicate the first datum to the first computing device with encryption and the second datum to the first computing device without encryption.*

The present invention is directed to an encryption module that encrypts only part of a message sent by one node to another node. By way of example, in one configuration of the present invention a graphical display is presented to a user requesting the user to input information into a number of input fields. Some of the fields require the entry of confidential information while others do not. The fields are identified accordingly. When user requests transmission of the displayed information to another node, the module encrypts only the confidential fields and not the non-confidential fields. The use of encryption on only part of the transmission can represent substantial savings in computational resources both at the transmitting and receiving nodes.

Herr-Hoymann et al. is directed to a method and apparatus for posting hypertext documents to a hypertext server so as to make the hypertext documents accessible to users of the hypertext document system while securing against unauthorized modification of the posted hypertext documents. The hypertext documents form a portion of the World Wide Web. The process for posting hypertext documents begins with an author authoring the hypertext pages on a client computer, sending an add request to a server computer, causing the generation of a unique identifier for the author of the document, obtaining a charge authorization from the author, and sending a database entry request from the client to the server including the unique identifier, the charge authorization, and the hypertext files, including the document. At the server, the validity of the charge authorization is verified, and if the charge authorization is valid the hypertext pages are stored in association with the unique identifier and the client is provided with a password needed to effect future modifications of the hypertext pages so published.

In rejecting the claims, the Examiner relies on the first datum being the credit card number (see element S7 of Figure 3) and the second datum being the elements, ID, data, and files sent with the credit card number in the e-Card create request from the author client 12 to the Linkstar server 18. At col. 4, lines 1-4, Herr-Hoymann et al. states as follows:

> At step S5, client 44 receives the unique ID and stores it as a local variable. Client 44 then requests a credit card number from the author (step S6), and encrypts the credit card number (step S7). In a preferred embodiment, public key encryption is used, wherein client 44 requests and receives from server 18 a public key for the encryption session. Client 44 uses the received public key to encrypt the credit card number.
>
> Once a credit card number is encrypted, client 44 creates an e-Card Create Request in the form of a multi-part message, such as shown by the example in Appendix D, and uploads the request to server 18 (step S8).

The silence of the text at col. 4, lines 1-16 on whether or not the non-credit card information in the request is encrypted is construed by the Examiner as an admission that it is not.

This conclusion, however, is not correct. At col. 6, lines 11-21, Herr-Hoymann et al. states that "GKEY - the client uses this message as part of a public key exchange for use in encrypting data *such as* the author's credit card number *or authorization data block.*" (Emphasis supplied.) The encryption referenced in this sentence appears to refer to encryption in the e-Card create request and not in the GKEY request. At col. 6, lines 11-21, Herr-Hoymann et al. discloses encrypting only the public key in the GKEY request. The authorization data block in the e-Card create request (Fig. 3) or SWUP message (Fig. 4) is believed to be the ID, data, and files. Even if the authorization data block is only the ID and data, nowhere does Herr-Hoymann et al. state that the files are not encrypted but in fact indicates that it is encrypted by using the open-ended phrases "such as." If the files were not encrypted, the purpose of the invention, namely the unauthorized changes of the files by imposters, could be compromised. Imposters could simply alter the unencrypted files during transmission.

This conclusion is supported by Appendix D. At column 4, lines 9-12, Herr-Hoyman et al. states that "[O]nce a credit card number is encrypted, client 44 creates an e-Card Create Request in the form of a multi-part message, such as shown by the example in Appendix D, and uploads the request to server 18 (step S8)." Appendix D "is an example of an uploading process of an e-Card and web pages as might occur in the process shown in Fig. 3 *between steps S2 and S9.*" (Page 24, lines 1-5.) (Emphasis supplied.) Thus, the example of Appendix D is made with reference to a sequence of steps that includes step S7, which is relied upon by the Examiner in rejecting the claims. At page 24, line 19, it is stated that "the following is uploaded to the script or file," which occurs between steps S8 and S9. The multipart upload itself is thereafter presented in Appendix D. As can be seen from page 24, the credit number and other information is shown as being in *plain text* (page. 24, lines 35-47). *Accordingly, the encryption must occur during the process of uploading the request to the server 18.* Because the request includes not only the credit card information but also the ID (e.g., page. 24, lines 49-52) and data and files (hypertext pages, e.g., page. 24, line 54-page. 32, line 35), *this means that not only the credit card information but also the ID, data, and attached files are encrypted prior to submission using the public key.*

Notwithstanding the foregoing, Herr-Hoymann et al. further fails to teach or suggest presenting a display to the user that includes fields for confidential and nonconfidential information and a procedure for distinguishing the confidential from the nonconfidential fields and respectively encrypting or not encrypting the information in the fields during later transmission of the information.

Huang et al. fails to overcome these deficiencies.

Accordingly, the pending claims are allowable over the cited references.

The dependent claims provide further reasons for allowance.

By way of example, dependent claim 2 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message and further includes the steps of providing a display to a user, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields; and receiving the message from the user, wherein the message corresponds to the display and wherein first datum refers to the first input field and the second datum to the second input field of the display. *See also* dependent Claim 16.

Dependent claim 3 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the steps of communicating the first datum with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message and the further steps of providing a display to a user, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields and receiving the message from the user, wherein the message corresponds to the display and wherein the first datum refers to the first input field and the second datum to the second input field of the display. *See also* dependent Claim 17.

Dependent claim 4 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claim 18.

Dependent claim 5 requires the step of employing the same path to communicate the first datum with encryption and the second datum without encryption to include the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claim 19.

Dependent claim 6 requires the step of communicating the first datum of the message with encryption of the first datum to include the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum. *See also* dependent Claims 7-9 and 20-22.

Dependent claim 10 requires the step of communicating a procedure from the second computing device to the first computing device, and wherein the step of communicating the first datum of the message from the first computing device to the second computing device with encryption of the first datum comprises the step of employing the procedure to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device. *See also* dependent Claims 11-14 and 23-27.

Dependent claims 30-35 are also allowable over the cited art for reasons noted above.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz
Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: Nov 10, 2004